

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-23420

(P2003-23420A)

(43)公開日 平成15年1月24日 (2003.1.24)

(51) Int.Cl. ⁷	識別記号	F I	マークト ⁸ (参考)
H 04 L 9/08		G 06 F 13/00	3 5 3 C 5 B 0 8 5
G 06 F 13/00	3 5 3		3 1 0 E 5 B 0 8 9
15/00	3 1 0	G 09 C 1/00	6 4 0 E 5 J 1 0 4
G 09 C 1/00	6 4 0		6 6 0 E 5 K 0 3 0
	6 6 0	H 04 L 12/56	A 5 K 0 6 7
			審査請求 有 請求項の数35 O L (全 18 頁) 最終頁に続く

(21)出願番号 特願2002-69405(P2002-69405)

(22)出願日 平成14年3月14日 (2002.3.14)

(31)優先権主張番号 60/278436

(32)優先日 平成13年3月26日 (2001.3.26)

(33)優先権主張国 米国 (US)

(31)優先権主張番号 10/057914

(32)優先日 平成14年1月29日 (2002.1.29)

(33)優先権主張国 米国 (US)

(71)出願人 000004237
日本電気株式会社
東京都港区芝五丁目7番1号

(72)発明者 イエンス-ピーター レドリッヒ
アメリカ合衆国, ニュージャージー
08540 プリンストン, 4 インディペン
デンス ウエイ, エヌ・イー・シー・ユ
ー・エス・エー インク内

(74)代理人 100097157
弁理士 桂木 雄二

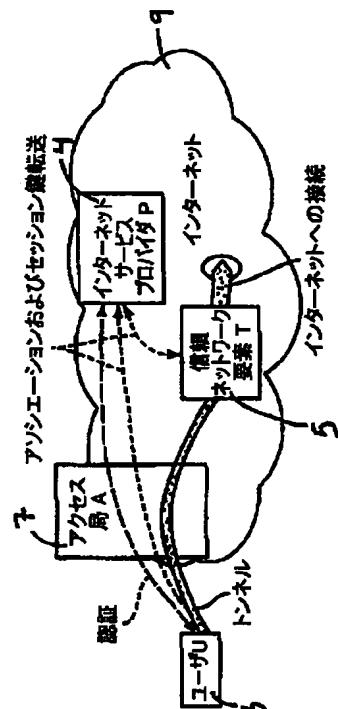
最終頁に続く

(54)【発明の名称】 信頼されないアクセス局を介した通信方法

(57)【要約】

【課題】 公衆インターネットやプライベートLANのようなパブリックまたはプライベートIPネットワークへのアクセスのために、既存のインフラストラクチャの共有を可能にするメカニズムを提供する。

【解決手段】 端末Uと非信頼アクセス局Aの間に接続を確立する。次に、端末Uと契約しているインターネットサービスプロバイダ (ISP) PへISP認証要求を送信する。ISP Pと端末Uが正しく認証された後、端末Uと信頼ゲートウェイTの間に信頼された接続を確立する。こうして確立される安全なトンネルにより、ISP Pは、端末Uに所定のサービスを提供するため、アクセス局Aにおけるリソースの制御を動的に取得することが可能となる。端末UとISP Pの正当な認証後、ISP Pは、データパケットを暗号化するためのセッション鍵を生成することも可能である。



【特許請求の範囲】

【請求項1】 ユーザの端末（U）とインターネットへの信頼ゲートウェイ（T）との間で非信頼アクセス局（A）を介して安全な通信を確立する通信方法において、

端末（U）と非信頼アクセス局（A）の間のアソシエーションを確立するステップと、

端末（U）からISP（P）へ前記非信頼アクセス局（A）を介してISP認証パケットを送信するステップと、

前記ISP（P）から前記端末（U）へ前記非信頼アクセス局（A）を介してユーザ認証パケットを送信するステップと、

前記ISPにおいて、

前記端末（U）と前記ISP（P）との認証後、前記端末（U）と信頼ゲートウェイ（T）との間のトライフィックを暗号化するために使用されるセッション鍵を生成するステップと、

前記セッション鍵を前記端末（U）および前記信頼ゲートウェイ（T）に配送するステップと、

前記端末（U）が前記信頼ゲートウェイ（T）を介してインターネットと通信することができるような安全なトンネルを確立するステップと、

を有し、

前記安全なトンネルは、前記端末（U）と前記インターネットの間で前記信頼ゲートウェイ（T）を介して送信されるトライフィックが、第三者の前記非信頼アクセス局（A）による変更または傍受から安全であるように、前記端末（U）と前記信頼ゲートウェイ（T）の間の物理リンクをエミュレートする、
ことを特徴とする通信方法。

【請求項2】 前記ISP認証パケットは、前記ISP（P）の身元を認証するための、前記端末（U）から前記ISP（P）への認証チャレンジ（CH...U）を含むことを特徴とする請求項1記載の方法。

【請求項3】 前記ユーザ認証パケットは、前記端末（U）のユーザの身元を認証するための、前記ISP（P）から前記端末（U）への認証チャレンジ（CH...P）を含むことを特徴とする請求項1記載の方法。

【請求項4】 非信頼アクセスポイントを有する非信頼インフラストラクチャを介してIPベースのネットワークへのパブリックアクセスを提供する方法において、IP装置（U）と前記非信頼アクセスポイント（A）の間に、IPアドレスが該IP装置に動的に割り当てられる接続を確立するステップと、

ISP認証要求を、前記IP装置（U）から、前記IP装置（U）が契約しているインターネットサービスプロバイダ（ISP）（P）へ、第三者所有の前記非信頼インフラストラクチャに所属する前記非信頼アクセスポイント（A）を通じて、送信するステップと、

前記IP装置（U）が前記ISP（P）と契約している正当なユーザであるかどうかを判断するためのユーザ認証要求を、前記ISP（P）から、前記IP装置（U）へ、前記第三者所有の非信頼インフラストラクチャに所属する前記非信頼アクセスポイント（A）を通じて、送信するステップと、

前記ISP（P）において、

前記ISP認証要求および前記ユーザ認証要求が正当であるとき、前記IP装置（U）と信頼ノード（T）の間で送信されるデータを暗号化するために使用される、データパケットを暗号化するためのセッション鍵を生成するステップと、

前記セッション鍵を前記IP装置（U）および前記信頼ノード（T）に配送するステップと、
を有し、さらに、

前記IP装置（U）とインターネットの間で非信頼アクセスポイント（A）を介して送信されるデータパケットが、安全なトンネルにおいて、前記非信頼アクセスポイント（A）による変更および操作から保護されるよう、前記IP装置（U）と前記信頼ノード（T）の間で送信されるデータパケットを暗号化するために前記セッション鍵が使用される安全なトンネルを確立するステップを有することを特徴とする、IPベースのネットワークへのパブリックアクセスを提供する方法。

【請求項5】 非信頼アクセス局（A）を有する第三者所有の非信頼インフラストラクチャを通じてIPベースのネットワークへのパブリックアクセスを提供する方法において、

IP装置（U）と前記アクセス局（A）の間に、IPアドレスが該IP装置に動的に割り当てられる接続を確立するステップと、

前記IP装置（U）が契約しているインターネットサービスプロバイダ（ISP）（P）へ、該ISP（P）が真正であることの証明を要求するISP認証要求を送信するステップと、

前記ISP（P）から前記IP装置（U）へ、前記IP装置（U）が前記ISP（P）とサービス契約を結んでいるかどうかを確認するためのユーザ認証要求を送信するステップと、

前記ISP（P）および前記IP装置（U）が正しく認証された後、前記IP装置（U）と信頼ゲートウェイ（T）との間に信頼された接続を確立するステップと、
を有し、

前記信頼された接続を通して、前記ISP（P）は、前記IP装置（U）に所定のサービスを提供するために、前記非信頼アクセス局（A）におけるリソースの制御を動的に取得可能であることを特徴とする、IPベースのネットワークへのパブリックアクセスを提供する方法。

【請求項6】 端末（U）と、該端末と契約しているインターネットサービスプロバイダ（P）と、インターネ

ットとの間に、第三者所有の非信頼アクセス局（A）を通じて安全な接続を確立する方法において、前記端末（U）と前記アクセス局（A）との間に接続を確立するステップと、前記端末（U）および前記インターネットサービスプロバイダ（ISP）（P）へISP認証要求を送信するステップと、前記ISP（P）および前記端末（U）が正しく認証された後、前記端末（U）と信頼ノード（T）との間に信頼された接続を確立するステップと、

を有し、

前記信頼された接続により、前記ISP（P）は、前記端末（U）に所定のサービスを提供するために、前記非信頼アクセス局（A）におけるリソースの制御を動的に取得可能であることを特徴とする、非信頼アクセス局を通じて安全な接続を確立する方法。

【請求項7】 前記ISP認証要求は、前記ISP（P）の身元を認証するための、前記端末（U）から前記ISP（P）への認証チャレンジ（CH_U）を含むことを特徴とする請求項6記載の方法。

【請求項8】 前記ユーザ認証要求は、前記端末（U）が前記ISP（P）のサービスに加入しているという身元を認証するための、前記ISP（P）から前記端末（U）への認証チャレンジ（CH_P）を含むことを特徴とする請求項6記載の方法。

【請求項9】 前記端末（U）および前記ISP（P）の正当な認証後、前記ISP（P）は、データパケットを暗号化するためのセッション鍵を生成することを特徴とする請求項6記載の方法。

【請求項10】 前記ISP（P）は、前記インターネットの前記信頼ノード（T）を選択することを特徴とする請求項6記載の方法。

【請求項11】 前記ISP（P）は、前記端末（U）および前記信頼ノード（T）に前記セッション鍵を配送することを特徴とする請求項9記載の方法。

【請求項12】 セッション鍵が、前記端末（U）と前記信頼ノード（T）との間で送信されるデータパケットを暗号化するために使用されることを特徴とする請求項6記載の方法。

【請求項13】 前記端末（U）と前記信頼ノード（T）との間での暗号化されたデータパケットの送信により安全なトンネルを確立することを特徴とする請求項12記載の方法。

【請求項14】 前記安全なトンネルは、前記非信頼アクセス局による操作からデータパケットを保護することを特徴とする請求項13記載の方法。

【請求項15】 前記信頼された接続の確立後、タイムアウト値が信頼ノード（T）および端末（U）に配送されることを特徴とする請求項6記載の方法。

【請求項16】 前記タイムアウト値は所定の期間に設定され、前記信頼された接続は、前記タイムアウト値に

等しい期間のあいだ有効であり、タイムアウト時には前記信頼された接続のために利用されたリソースが解放される、ことを特徴とする請求項15記載の方法。

【請求項17】 前記信頼ノード（T）は、前記端末（U）から暗号化されたデータパケットを受信した後、該データパケットを復号し、復号されたデータパケットをインターネットに転送することを特徴とする請求項6記載の方法。

【請求項18】 前記信頼ノード（T）は、前記端末（U）から暗号化されたデータパケットを受信した後、該データパケットを復号し、復号されたデータパケットをリモート通信相手（R）に転送することを特徴とする請求項17記載の方法。

【請求項19】 前記インターネットは、前記信頼ノード（T）を介して前記端末（U）へもとのデータパケットを送信し、前記信頼ノード（T）は、もとのデータパケットを暗号化し、暗号化されたデータパケットを、前記非信頼アクセス局（A）を介して前記端末（U）に転送することを特徴とする請求項18記載の方法。

【請求項20】 前記端末（U）は、前記信頼ノード（T）から暗号化されたデータパケットを受信した後、セッション鍵を利用して該データパケットを復号することにより、インターネットからのもとのデータパケットを得ることを特徴とする請求項17記載の方法。

【請求項21】 前記リモート通信相手（R）が、前記信頼ノード（T）を介して前記端末（U）へもとのデータパケットを送信し、前記信頼ノード（T）は、もとのデータパケットを暗号化し、暗号化されたデータパケットを、前記非信頼アクセス局（A）を介して前記端末（U）に転送することを特徴とする請求項18記載の方法。

【請求項22】 前記端末（U）は、前記信頼ノード（T）から暗号化されたデータパケットを受信した後、セッション鍵を利用して該データパケットを復号することにより、前記リモート通信相手（R）からのもとのデータパケットを得ることを特徴とする請求項21記載の方法。

【請求項23】 前記ISP（P）は、前記端末（U）によって利用されたリソースについて、前記非信頼アクセス局（A）に時間のアカウンティングを提供することを特徴とする請求項6記載の方法。

【請求項24】 前記非信頼アクセス局（A）は、第三者所有のネットワークインフラストラクチャに組み込まれていることを特徴とする請求項6記載の方法。

【請求項25】 前記ISP（P）は、前記非信頼アクセス局（A）を介して、少なくとも1つの加入サービスを前記端末（U）に提供することを特徴とする請求項24記載の方法。

【請求項26】 前記ISP（P）は、時間のアカウンティングに従って、前記端末（U）に対して費やされた

リソースについて、前記非信頼アクセス局（A）に償還することを特徴とする請求項6記載の方法。

【請求項27】 前記ISP（P）は、前記端末（U）に提供されたサービスについて当該端末（U）に課金することを特徴とする請求項25記載の方法。

【請求項28】 前記非信頼アクセス局（A）は、公共施設のネットワークインフラストラクチャ内に位置することを特徴とする請求項24記載の方法。

【請求項29】 前記公共施設は、空港、会議場、レストラン、ホテル、図書館、および学校のうちの少なくとも1つであることを特徴とする請求項28記載の方法。

【請求項30】 前記非信頼アクセス局（A）は、私宅のインフラストラクチャ内に、または、企業もしくは政府機関の私設インフラストラクチャ内に位置することを特徴とする請求項24記載の方法。

【請求項31】 前記非信頼アクセス局（A）は、 WLAN（IEEE802.11）、Bluetooth（IEEE802.15）、またはHyperLanを含む少なくとも1つのワイヤレス伝送標準と互換であることを特徴とする請求項6記載の方法。

【請求項32】 前記端末（U）はモバイル装置であることを特徴とする請求項6記載の方法。

【請求項33】 前記端末（U）は、動的ホスト設定プロトコル（DHCP）要求をプロードキャストし、前記非信頼アクセス局（A）から「マジック」DHCP応答を受信することによって、互換アクセスポイントを認識することを特徴とする請求項6記載の方法。

【請求項34】 前記非信頼アクセス局（A）は、同時に複数の端末（U）にサービスするときには、端末とデータパケットとのマッチングを容易にするために、ローカル固有識別（LUID）を端末（U）に割り当てるこことを特徴とする請求項6記載の方法。

【請求項35】 非信頼アクセスポイントを介してインターネットサービスのアクセスおよび認証を行うコンピュータプログラム製品において、コンピュータに所定の動作を実行させるソフトウェア命令と、

前記ソフトウェア命令を保持するコンピュータ可読媒体と、を有し、

前記所定の動作は、

IP装置（U）とアクセス局（A）の間に、IPアドレスが該IP装置（U）に動的に割り当てる接続を確立するステップと、

前記IP装置（U）が契約しているインターネットサービスプロバイダ（ISP）（P）へ、該ISP（P）が真正であることの証明を要求するISP認証要求を送信するステップと、

前記ISP（P）から前記IP装置（U）へ、前記IP装置（U）が前記ISP（P）とサービス契約を結んでいるかどうかを確認するためのユーザ認証要求を送信す

るステップと、

前記ISP（P）および前記IP装置（U）が正しく認証された後、前記IP装置（U）と信頼ゲートウェイ（T）の間に信頼された接続を確立するステップとを含み、

前記信頼された接続により、前記ISP（P）は、前記IP装置（U）に所定のサービスを提供するために、信頼されない第三者所有の前記アクセス局（A）におけるリソースの制御を動的に取得可能であることを特徴とする、非信頼アクセスポイントを介してインターネットサービスのアクセスおよび認証を行うコンピュータプログラム製品。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はIPネットワークへのパブリックアクセスを提供するシステムに係り、特に、第三者所有の信頼されない（非信頼）アクセソードを通じて、インターネットサービスプロバイダがその加入者にインターネットアクセスを提供する際の通信方法に関する。

【0002】

【従来の技術】 下記の文献は、ワイヤレス技術に関する有用な背景的知識を提供する。

【0003】 1) Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd Edition, John Wiley & Sons, 1995, ISBN 047117099.

【0004】 2) R. Droms, "Dynamic Host Configuration Protocol (DHCP)", IETF RFC 2131, 1997.

【0005】 3) Egevang, K. and Francis, P., "The IP Network Address Translator (NAT)", IETF RFC 1631, 1994.

【0006】 本発明は、第三者が運営するアクセス局を用いて、公衆インターネット、社内インターネット、あるいはプライベートLANのようなIPネットワークへのパブリックアクセスを提供するシステムおよび方法において、ユーザも、このユーザのISPも、いずれもそのアクセス局の正確なオペレーションを信頼していないため、そのアクセス局が「非信頼」アクセス局となっているような場合のシステムおよび方法に関する。より具体的には、本発明は、悪意のある可能性があり、それゆえ信頼されない（非信頼）第三者によって運営されるアクセス局を介してIPネットワークにアクセスするためには、データの認証(authentication)、権限付与(authorization)、アカウンティング(accounting)、および暗号化を実行する方法に関する。本発明の方法およびシステムは、ワイヤレス（無線）およびワイヤライン（有線）のアクセスに関して同様に使用可能である。ここで、「ワイヤレス」とは、無免許周波数帯で動作する短距離技術であることも、より長距離の免許を受けた電波技術

であることも可能である。

【0007】インターネットのようなIPネットワークへの従来技術のパブリックアクセスは、インターネットサービスプロバイダ（ISP）を通じて提供されている。ISPは、モデムのような伝送設備も所有またはリースする。ほとんどの場合、インターネットにアクセスしたいユーザは、与えられた地域エリアのISPとサービス契約を締結しなければならない。移動する加入者にサービス範囲を拡大するため、一部のISPは、認証、権限付与およびアカウンティングの手続きを管理するローミング契約を結んでいる。同様の手続きは、セルラ事業者についても行われ、与えられた事業者の加入者が別の事業者のカバレジエリアに移動することを可能している。しかし、これらの確立された手続きは、ネットワークアクセスが信頼できることを仮定している。この仮定は、ダイヤルアップモデムバンクのようなプライベートアクセスメカニズム、インフラストラクチャの高いコスト、および、セルラ事業者の場合の周波数スペクトルの排他的所有によって保証されていた。

【0008】無免許周波数スペクトルで運営される安価なインフラストラクチャを用いてIPネットワークへのワイヤレスアクセスを可能にする第2の従来技術の出現は、小規模の独立系アクセスプロバイダの新設を容易にしている。ワイヤレスローカルエリアネットワーク（ WLAN）およびパーソナルエリアネットワーク（PAN）に基づくそれらのワイヤレスアクセス技術の到達範囲は小さいため、与えられた地所における公衆インターネットアクセスのためのインフラストラクチャの運営は、その地所の所有者によって管理される。実際、ケーブルやDSLを通じての高速インターネットアクセスを有するアパートや家屋の所有者であれば、WLANアクセスポイントを運営することによって、近隣にアクセスを提供することができる。しかし、そのようなワイヤレスアクセスポイントへのアクセスは、同じ組織あるいは家庭の装置に制限される。外来のIP装置（例えば、自分のWLANカードを装備した訪問者や、WLANカードを装備したPCを持っている隣人）にアクセスを提供することは安全（セキュア）でなく、通常は許可されず、技術的に不可能なこともある。さらに、私有のアクセス局は通常、その所有者のISPに接続されている。すなわち、別のISPに加入したゲストは、自分のISPによって提供されるサービスを取得することができず、インターネットアクセスのために自分のISPによって課金されることもできない。

【0009】

【発明が解決しようとする課題】上記第1の従来技術として説明したパブリックアクセスを可能にするメカニズムを、上記第2の従来技術として説明した小さい地理的エリアにおけるインターネットアクセスを提供する小規模独立系事業者に適用することは、さまざまな問題点お

より欠点を有する。例えば、ローミングユーザは、WLANの事業者の信頼性を知らない。悪意のある事業者が、ユーザとコンテンツプロバイダの間の通信を傍受するのが容易であることを発見するかもしれない。そのような事業者は、ユーザのトラフィックからログイン名やパスワードのような資格証明を取得する手段を見つける可能性もある。さらに、従来技術の認証および権限付与の手続きでは、使用量に基づくアカウンティングが容易でない。これは、ローミングユーザに提供されるアクセスについての独立系事業者の精算のために必要となる。

【0010】今日、私有のアクセス局は至る所で利用可能であり、インターネットにアクセスする潜在的手段をどこにいるユーザにも提供している。しかし、現在のISPは、自分でインフラストラクチャを構築しなければならず、これは、一時的ユーザをサポートすることに関しては高価であり、しばしば融通性に欠ける。

【0011】本発明の目的は、第三者所有の信頼されない（非信頼）アクセソードを通じて、インターネットサービスプロバイダがその加入者にインターネットアクセスを提供する安全な方法を提供することである。

【0012】本発明のもう1つの目的は、インターネットサービスプロバイダとアクセソード所有者の間、および、インターネットサービスプロバイダと加入者との間で、アカウンティング情報を提供することである。このアカウンティング情報は、システムの動作の一体をなす部分として導出され、悪意のある操作から保護される。

【0013】

【課題を解決するための手段】本発明は、IPネットワークへのアクセス局に関する。具体的には、本発明は、そのサービスのユーザおよびこのユーザのISP以外の当事者によって所有され運営される、IPネットワークへのアクセス局に関する。さらに具体的には、本発明は、コンピュータなどのIPベースの装置に、例えばインターネットや社内インターネットのようなIPネットワークへのアクセスを提供することができる装置に関する。この場合、アクセス局は、サービスを希望するIP装置から、ユーザの識別とユーザのISPの識別とを取得する。アクセス局は、サービスを取得したいというユーザの希望についてユーザのISPに通知する。ユーザのISPは、ユーザが加入したサービスを提供するために、アクセス装置内のリソースの制御を動的に取得する。最後に、ISPは、そのリソースの使用量に対するアクセス局の支払いを手配し、ユーザ（その加入者）の課金を手配する。

【0014】本発明は、インターネットサービスプロバイダでインターネットサービスに加入したエンドユーザ、アクセソードあるいはインフラストラクチャの所有者、および、インターネットへの信頼されるゲートウェイ、ならびに、第三者所有のアクセソードを通じて

インターネットサービスの加入者に匿名インターネットアクセス提供を行う方法を含む。具体的には、本発明は、加入者とインターネットサービスプロバイダとの相互認証の手続き、および、エンドユーザーとインターネットへの信頼ゲートウェイとの間の安全なトンネルの確立に必要な鍵配送とを含む。本発明の方法は、サービス要求のステップと、インターネットサービスプロバイダ認証のステップと、加入者認証のステップと、一意的なセッション鍵を生成するステップと、セッション鍵を信頼されるネットワークノードおよび加入者に配送するステップと、前に配送されたセッション鍵を用いて第三者アクセスノードを通じて加入者と信頼されるネットワーク要素との間に確立される安全なトンネルを用いてデータ転送を行うステップとを含む。

【0015】本発明の方法は、さらに、インターネットサービスプロバイダから加入者、アクセスノードおよび前記信頼されるネットワーク要素にタイムアウト値を配達するステップを含む。タイムアウト値は、前記加入者とインターネットサービスプロバイダの間の再認証手続きをトリガする。

【0016】さらに、本発明の方法は、加入者および信頼されるネットワーク要素に配置される、トンネルに関するタイマと、前記アクセスノードに配置される別のタイマのうちの1つが満期になった場合に、トンネルを解放するステップを含む。

【0017】さらに、成功した認証の数に基づいてアカウンティング情報を生成する方法が提供される。アカウンティング情報を用いてプリペイドサービスを提供し、再認証前の残り時間を判定する方法も提供される。

【0018】本発明の応用分野としては以下の場合があるが、もちろん、これらに限定されるものではない。

- ・個人の家庭内のアクセス局が、WLAN (IEEE 802.11)、Bluetooth (IEEE 802.15)、あるいはHiperLANに基づくワイヤレスアクセスを訪問者や近隣に提供する場合。

- ・ホテルや空港が、その顧客のISPによって管理されるインターネットアクセスを顧客に提供するために、アクセス局 (WLAN、Bluetooth、HiperLAN) を所有し運営する場合。

- ・会議が、会議参加者に、その会議参加者のISPによって管理されるインターネットアクセスを与えるために、会議開催地でアクセス局 (WLAN、Bluetooth、HiperLAN) をリースし一時的に配備する場合。

【0019】理解されるべき点であるが、明細書全体を通じて、「インターネット」という用語は、その最広義における「IPに基づくネットワーク」を意味し、これには、公衆インターネット、社内インターネット、プライベートまたはパブリック (公衆) LAN、およびIPベースのアドホックネットワークが含まれるが、これら

には限定されない。

【0020】

【発明の実施の形態】以下、本発明の好ましい実施例について、図面を参照して説明する。

【0021】以下の詳細な説明は、次のように構成される。「コンポーネントの概観」と題するセクションでは、システムのコンポーネントを紹介し、コンポーネントの相互関係の説明を行う。「本発明の動作」と題するセクションでは、本発明のさまざまな実施例と、その応用について説明する。さらに、理解と明確さを促進するために、本発明の説明は、「UとPの相互認証」、「アクセス局A (7) を通じての端末U (3) と信頼ノードT (5) の間の安全なトンネル (1) の作成」、「端末UとIPネットワークの間のデータ転送」、「トンネル解放とタイムアウト」、「課金」の各セクションに分けられる。

【0022】【コンポーネントの概観】再度注意を喚起しておくが、「IPネットワーク」という用語は、公衆インターネットおよび社内インターネットを含む、すべての可能なIPベースのインフラストラクチャネットワークを表すために用いられる。

【0023】ユーザの端末装置 (U)

Uは、ユーザのIPベースの端末装置を表す。これは、インターネットプロトコルスイート (IP) を用いて他の装置と通信する移動式あるいは固定式の装置である。これには、ワークステーションコンピュータ、パーソナルコンピュータ (PC)、ラップトップコンピュータ、ハンドヘルドPC、電話機あるいはその他のIPベースの装置あるいは機器が含まれるが、これらには限定されない。しかし、予想されるように、ほとんどの場合、この端末装置は、小型で移動式のものであり、IPネットワークに接続するための有線またはワイヤレスの一方または両方の手段を有することになる (下記の「アクセス局」参照)。さらに、与えられた任意の時刻において、この装置は、高々1ユーザに関連づけられる、すなわち、「このユーザの装置」として認識できることが仮定される。

【0024】アクセス局 (A)

Aは、アクセス局を表す。アクセス局は、端末装置UをIPベースのインフラストラクチャネットワーク (例えば、インターネットやインターネット) に接続するためには使用される。アクセス局は、IPネットワークからトラフィックを受け取り、それを正しい端末Uに配信するとともに、端末Uからトラフィックを受け取り、それをIPネットワークに転送する。AとUの間の通信の手段は、有線でも無線でもよい。本発明は、両方の場合に適用がある。さらに、Aは、所有者および運営者を有するとともに、例えば、ある周波数スペクトルを使用する許可を必要とする無線基地局 (ベースステーション) の場合には、運営特権の所有者を有する。本明細書の目的の

ために、これらのすべての側面をAという抽象概念にまとめる。

【0025】通常、アクセス局Aは、IPネットワークに常時接続されるが、アクセス局Aと端末Uの間の接続は本来一時的である。例えば、アクセス局Aは、公共エリア（例えば、ホテル、空港、レストラン）に配置されることも、非公共エリア（例えば、個人の家庭内）に配置されることも可能である。後者の場合、アクセスは、物理的にアクセス可能なユーザ（例えば、Aの所有者の訪問客）に制限されてもよく、あるいは、アクセスは、Aの通信範囲内のすべてのユーザに利用可能であるとしてもよい（例えば、Aは、Aの近隣および訪問者にインターネットアクセスを提供するために利用可能な、私宅内の802.11/Bluetooth/HiperLan基地局である）。

【0026】インターネットサービスプロバイダ（P）
Pは、インターネットサービスプロバイダ（ISP）を表す。ISPは、サービスパラメータを規定するUとPの間の加入契約に基づいて、サービスを端末装置Uに提供する。このため、Pは、エンドユーザサービスについてUに課金する責任があると仮定することができる。また、Pは、Aのリソースを使用することについて、Aに支払いをしなければならないと仮定することもできる。また、Uとその通信相手との間のトラフィックが、Aからのパケットのスヌーピング／挿入／変更あるいはその他の攻撃に対して安全であることを保証することも、Pの責任である。

【0027】通常、Pは、収益をあげるために、個人あるいは他の会社にインターネットアクセスおよびその他の関連サービス（例えば、電子メール）を提供する会社である。もう1つの可能性として、Pは、その従業員にIPネットワーク（例えば、社内インターネット、公衆インターネット、あるいはプライベートIPネットワーク）へのアクセスを提供する会社である。ここでは、主要な目標は、直接的に収益をあげることではなく、従業員の作業プロセスのサポートである。例えば、FedExの従業員は、時折社内IPネットワークにアクセスして、荷物を配送したことについて社内データベースを更新する。

【0028】信頼ネットワーク要素（T）

Tは、信頼されるネットワーク要素を表す。Tは、Tが端末装置Uとの間のトラフィックに対するスヌーピング／挿入／変更の手段をAに提供しないという限りで、Pにとって信頼できると判断する、インターネット内のルータである。本発明は、いったんトラフィックがインターネットコアに到達したら、そのトラフィックは、悪意のある攻撃に対して相当に安全であると仮定する。その理由は、この場合、ネットワークは少数の、定評のある、信頼された長距離会社のみによって運営されているからである。

【0029】異なるISPは、Tが信頼される要素であるかどうかを判断するために、おそらくはそのユーザの要求およびUの現在位置に依存して、異なるメカニズムおよびポリシーを適用することがある。Pが、インターネット内の信頼できるルータについての知識を有しない場合、P自体がTの役割を受け持つ、すなわち、Pは自分のルータのうちの1つをTとして選択すると仮定される。

【0030】リモート通信相手（R）

Rは、リモート通信相手を表す。リモート通信相手は、端末Uが通信を要求する相手となる任意のリモートホストであることが可能である。例えば、リモート通信相手Rには、公衆インターネット上のサーバおよびその他のIPベースの装置、社内インターネット上のサーバ、あるいは、社内インターネットやプライベートIPネットワーク内のワークステーションやパーソナルコンピュータが含まれるが、これらには限定されない。

【0031】仮定

本発明の目的のため、コンポーネントUとAの間は、AとPの間とともに、互いに信頼関係がないと仮定される。具体的には、端末装置Uがリモート相手側Rと通信したいとき、Uは、Pからサービスを取得するために、単にその近傍内のアクセス局Aを探索するだけである。通常、Uは、AとUの間に信頼を生じるような長期間継続する関係をAとの間で有することはない。

【0032】さらに、アクセス局Aは、UやPを信頼しないと仮定される。アクセス局Aの主要な関心は、アクセス局Aによって端末Uに提供されたリソースおよびサービスに対する償還を取得することに集中される。

【0033】最後に、Pは、アクセス局Aを信頼しない。Pは、その加入者Uが、Aによって要求されたように実際にAのリソースを使用していることを保証しなければならない。これは、アクセス局Aが、存在しない端末UをPに報告し、おそらくはUからの虚偽のトラフィックさえ生成するような状況を回避するためである。そのような状況では、Pは、AがPの真の加入者にサービスしていないのにAに補償をすることになってしまふ。AによってUに対してなされるサービスについてのPとAの間の支払い手続きは、好ましくは、関連する当事者間の精算契約によって管理される。前述のように、UとPの間の支払い手続きは、サービス契約によって管理され、定額制料金、あるいは、時間単位やトラフィック量単位で決定される使用料金に基づくことが可能である。

【0034】本発明の応用

本明細書では、第三者所有のインフラストラクチャを通じてIPネットワーク（例えば、公衆インターネットや社内インターネットのような）へのパブリックアクセスを提供するシステムおよび方法は、当業者には明らかのように、いくつかの具体的な方法で実現される。具体的には、本発明のシステムおよび方法は、全体として、ハ

ードウェア、ソフトウェアまたはその両方の組合せとして実現される。特に、本発明によって利用されるアクセスポイントあるいはその他のハードウェア要素は、プロセッサと、そのプロセッサの制御下にあるメモリとを有する。メモリには、プロセッサによって実行される命令（ソフトウェア）が提供され、これにより、プロセッサは、アクセス局、あるいはその他のハードウェアをさまざまな方法で動作させることができ可能となる。同様に、アクセス局は、部分的に、ハードウェアおよびソフトウェアとして実現可能である。

【0035】また、IPネットワークへのアクセスを提供する本発明のシステムおよび方法は、ワイヤレスおよび有線のアクセスに関して同様に使用可能である。ここで、「ワイヤレス」とは、無免許周波数帯で動作する短距離技術を意味することも、より長距離の免許を受けた電波技術を意味することも可能である。

【0036】さらに、IPネットワークへのパブリックアクセスを提供する本発明のシステムは、IPネットワークに接続するための有線、ワイヤレスまたはそれらの組合せの手段のいずれを用いて実現することも可能である。したがって、理解されるべき点であるが、「IPネットワーク」あるいは「インターネット」という用語は、その最広義における「IPに基づくネットワーク」を意味し、これには、公衆インターネット、社内インターネット、プライベートまたはパブリックLAN、およびIPベースのアドホックネットワークが含まれるが、これらには限定されない。

【0037】第三者のインフラストラクチャを用いて（インターネットのような）IPネットワークへのアクセスを提供する本発明のシステムおよびメカニズムの利点は、ISPにとって利用可能であるとともに、自己の通信の必要のためにインターネットを使用する企業にも利用可能である。本発明の1つの利点は、ISP/会社が、自己のアクセスネットワークを必要としないことである。したがって、ISP/会社は、広い地域をアクセスポイントでカバーすることや、免許を要する周波数スペクトルのために高額な免許を取得する必要がない。

【0038】本発明のシステムの例示的な応用分野には、以下の場合があるが、これらには限定されない。

- ・個人の家庭内のアクセス局が、WLAN (IEEE 802.11)、Bluetooth (IEEE 802.15)、あるいはHyperLanなどの（これらには限定されない）ワイヤレス伝送標準を用いて、ワイヤレスアクセスを訪問者や近隣に提供する場合。
- ・ホテルや空港のような第三者によって所有され運営されるネットワークインフラストラクチャ内に実現された公共エリアアクセス局が、顧客のISPによって管理されるインターネットアクセスを顧客や訪問者に提供する場合。実現のためのワイヤレス標準には、WLAN (IEEE 802.11)、Bluetooth (IEEE

802.15) およびHyperLanが含まれるが、これらには限定されない。

・アクセス局が、一時的に配備されリースされる場合。例えば、会議が、会議参加者に、その会議参加者のISPによって管理されるインターネットアクセスを与えるために、会議開催地でアクセス局をリースすることがある。実現のためのワイヤレス標準には、WLAN (IEEE 802.11)、Bluetooth (IEEE 802.15) およびHyperLanが含まれるが、これらには限定されない。

【0039】パブリックアクセスLAN環境に複数のワイヤレスアクセス技術を提供するため、さまざまなワイヤレス製品およびさまざまなタイプのワイヤレス事業者が共存可能であり、したがって、本発明の実施例は、さまざまなベンダからのワイヤレスLANカードとは独立の、相互運用可能なエアインターフェースであることに注意すべきである。

【0040】【本発明の構成および動作】図1に本発明のコンポーネントを利用可能なネットワークを例示する。図1に示されるように、安全な（セキュア）トンネル（1）（破線で表す）が、端末ユーザU（3）と信頼されるノードT（5）の間で、アクセス局A（7）を通じて確立される。いったん端末U（3）およびISP P（4）が認証されると、ISP Pは、信頼ノードT（5）を選択し、セッション鍵を端末U（3）および信頼ノード（5）に配達する（ISP（4）、端末（3）および信頼ノードT（5）の間の破線で表す）。この秘密のセッション鍵は、アクセス局Aには未知であるが、UとTの間の暗号化を容易にするために使用されることになる。アクセス局A（7）がデータをUからTへおよびTからUへ転送する能力とともに、UとTの間の安全なトンネル（1）を確立することができる。この安全なトンネル（1）を用いて、端末U（3）は、暗号化されたデータパケットを信頼ノードT（5）に送信することができる。信頼ノードT（5）は、破線で表されるように、データパケットをIPネットワーク（9）へ、特に、リモートホスト（10）へ転送する。

【0041】図2は、安全なトンネル（1）の確立に必要な、端末U（3）、アクセス局A（7）、ISP P（4）および信頼ノードT（5）の間の認証およびセッション鍵転送を示す同様のネットワークの図である。具体的には、端末U（3）およびISP P（4）は、両端に矢印のある長い破線で示されるように、アクセス局A（7）を通じて認証チャレンジを互いに送信する。端末U（3）およびISP P（4）の両方の正しい認証の後、ISP P（4）は、セッション鍵を生成し、短い破線で示されるように、信頼ノードT（5）および端末U（3）に配達する。このセッション鍵を用いて、端末U（3）および信頼ノードT（5）は、データメッセージを暗号化し、アクセス局A（7）を通る安全なトン

ネル（1）を通じてそれを転送する。しかし、データパケットの暗号化のため、アクセス局A（7）は、そのデータパケットを復号したり変更したりすることはできない。換言すれば、信頼ノードT（5）がデータパケットをIPネットワーク（9）との間で転送し受信する間、アクセス局A（7）は単に端末U（3）と信頼ノードT（5）の間の通路として作用するだけである。

【0042】UとPの相互認証

端末U（3）は、アクセス局A（7）にアクセスすることができる（すなわち、端末U（3）とアクセス局A（7）が、選択された通信媒体（有線またはワイヤレス）を通じてデータを交換することができる）地点に、スイッチオフモードで到着すると仮定する。さらに、端末U（3）およびISP-P（4）は、公開鍵基盤[Pub Key]に参加していると仮定する。具体的には、公開鍵基盤への参加者は、「公開鍵」および「秘密鍵」という2つの鍵を有する。秘密鍵は、その参加者のみが知っており、他の当事者には決して明かされない。公開鍵は、誰もがどの参加者の公開鍵をも知っているように公開される。文献“Applied Cryptography: Protocols, Algorithms, and Source Code in C”で説明されている理由により、このような鍵は、一方の鍵（公開鍵または秘密鍵）で暗号化されたデータは他方の鍵（それぞれ、秘密鍵または公開鍵）では復号することができるが、他の鍵ではできないという性質を有する。

【0043】次に、図2および図4を参照して、ユーザ端末U（3）が、たまたま端末U（3）の現在位置の近くにある信頼されないアクセス局A（7）を用いて、自己のISP-P（4）に対してどのようにしてサービスを要求するかについて説明する。

【0044】ステップS1において、端末U（3）が起動され、そのネットワークインターフェースが初期化されると、端末U（3）はIPアドレスを取得するためにDHCP（動的ホスト設定プロトコル）要求をネットワークにブロードキャストする。アクセス局A（7）は、このブロードキャストの範囲内にある場合、このDHCP要求を受信することになる。DHCPは、コンピュータやワークステーションが、中央のサーバによって管理されるプールから一時的または永続的なIPアドレスを得ることを可能にするIPベースのプロトコルである。通常、ホストネットワークはDHCPサーバを動作させ、一方、ワークステーションやモバイル装置はDHCPクライアントを動作させる。DHCPによれば、IPアドレスを（モバイル装置のような）ノードにオンザフライで動的に割り当てることが可能となる。DHCPに関する技術情報および背景的知識については、R. Dromsの“Dynamic Host Configuration Protocol (DHCP)”と題する文献を参照。注意すべき重要な点であるが、端末U（3）がアクセス局A（7）と通信するために使用する技術に依存して、端末U（3）は、DHCP要求をブロ

ードキャストする前に、アクセス局（7）とのある形式のアソシエーション（関連づけ）を作成することが必要な場合がある。このようなアソシエーションを確立する手続きは、IEEE802.11技術に関する関連文書に規定されている。

【0045】ステップS2において、アクセス局A（7）が本発明のメカニズムをサポートする場合、アクセス局A（7）は、「マジックDHCP応答」(magic DHCP response)により端末U（3）に応答する。端末U（3）がどのようにして「マジック」と「非マジック」（標準）のDHCP応答を区別するかについては後述する。「マジックDHCP応答」の目的は、端末U（3）に対して、アクセス局A（7）が本発明のメカニズムと互換性があることを示すことである。端末U（3）が標準なわち非マジックDHCP応答を受け取った場合、端末U（3）は、DHCPの標準の動作モードに従ってIPアドレスを取得するだけであるため、本発明のメカニズムは利用可能ではないことを知る。いずれの場合でも、DHCP応答は、アクセス局A（7）のIPアドレス（ゲートウェイとして識別される）と、端末U（3）のIPアドレス（クライアントIPアドレスとして識別される）を含む。

【0046】DHCP応答は、さまざまな方法で、「マジックDHCP応答」として定義されることが可能であり、それらはすべて、本発明の技術的範囲内に入る。例えば、DHCP応答は、値「1」に初期化された「AP」DHCPオプションフィールドを含む場合に、「マジックDHCP応答」とみなすことが可能である。DHCPプロトコルは、新たなオプションフィールドの動的な導入を見込んでいる。「AP」DHCPオプションフィールドの値が1であることは、端末U（3）が接続しようとしているアクセス局A（7）が、本発明のメカニズムをサポートすることを示す。他方、「AP」DHCPオプションフィールドがないか、1以外の値であることは、アクセス局A（7）が本発明のメカニズムをサポートしないことを示す。

【0047】別法として、「マジックDHCP応答」は、予約されたIPアドレスを端末Uに割り当てるDHCP応答として定義されることも可能である。例示のみの目的であるが、IPアドレス138.15.103.220（これは一般にNEC USAの管理下にある）を、この目的のために使用可能である。このIPアドレスはNEC USAに割り当てられているため、他のネットワークによってDHCPクライアントに割り当たれることはできない。NEC USAもまた、このアドレスを他の目的のために使用しないことを保証する。それゆえ、IPアドレス138.15.103.220が端末U（3）に割り当たることは、アクセス局A（7）が本発明のメカニズムをサポートすることを示す。他方、138.15.103.220以外のIPア

ドレスが端末U (3) に割り当てられることは、アクセス局A (7) が本発明のメカニズムをサポートしないことを示す。

【0048】端末U (3) が単に動的に割り当てられたIPアドレスすなわち「非マジック」DHCP応答を受け取るだけである場合、端末U (3) には、ネットワークおよびアクセス局A (7) が本発明をサポートしないことが確認される。したがって、端末U (3) は、第三者所有の信頼されないアクセス局A (7) を通じて、端末U (3) のISP P (4) を利用したインターネットアクセスを取得することはできない。

【0049】ステップS3aにおいて、端末U (3) は、アクセス局A (7) が存在すること、および、アクセス局A (7) が本発明のメカニズムをサポートすることを知ると、識別パケットをアクセス局A (7) に送る。このパケットは次のものを含む。

- ・端末U (3) が契約しているISPのIPアドレス。
- ・契約しているISP P (4) によって端末U (3) に以前に割り当てられた識別文字列あるいは番号。
- ・ISP P (4) を、端末U (3) が契約しているISPであるとして認証するために、端末U (3) によってランダムに生成されたチャレンジCH_U。

【0050】ステップS3bにおいて、アクセス局A (7) は、ISP認証パケットを端末U (3) から受け取ると、ローカル固有識別(LUID: local unique identification)を端末U (3) に割り当てる。LUIDは、アクセス局A (7) が同時に複数の端末Uにサービスしているような状況で、メッセージやデータパケットを正しい端末U (3) と関連づける(照合する、組み合わせる)ために、アクセス局A (7) によって利用される。LUIDは、アクセス局A (7) が正しい端末Uにデータを送信するのを助ける区別可能な識別属性であればよい。例として、LUIDは、端末U (3) のMACアドレスとすることが可能であるが、これには限定されない。

【0051】次に、アクセス局A (7) は、修正されたISP認証パケットをISP P (4) に転送する。アクセス局A (7) は、端末UのISP P (4) のIPアドレスを知っている。これは、ステップS (3a) で端末U (3) からアクセス局A (7) に送られたISP認証パケットに、端末U (3) によって含められていたからである。修正されたISP認証パケットは次のものを含む。

- ・アクセス局A (7) のIPアドレス (ISP P (4) がデータをアクセス局A (7) に転送することができるようになるため)。
- ・端末U (3) に割り当てられたLUID。
- ・端末U (3) の識別番号。
- ・端末U (3) がランダムに生成したチャレンジCH_U。

【0052】明確にしておかなければならない点であるが、端末U (3) の識別番号と端末U (3) のLUIDは2つの異なる無関係のIDである。識別番号は、ISP P (4) によって前もって端末U (3) に割り当てられたものである(例えば、これは、端末U (3) とISP P (4) が加入契約を結んだときに決定されたユーザ名である)。これに対して、LUIDは、アクセス局A (7) によって端末U (3) に動的に割り当てられ、アクセス局A (7) が現在サービスを提供している端末U (3) を列挙するためにアクセス局A (7) のみによって使用されるものである。端末U (3) およびISP P (4) のいずれも、アクセス局A (7) がどのようにしてLUIDを選択し割り当てるかには影響を及ぼさない。

【0053】ステップS4aにおいて、ISP P (4) は、アクセス局A (7) から修正されたISP認証パケットを受け取ると、アクセス局A (7) を通じてインターネットあるいはその他のサービスを取得することを端末U (3) が要求していることを知る。しかし、ISP P (4) は、ISP認証パケットの発信者が正当な端末U (3) でありISP P (4) と契約しているかどうかを確かめることができない。例えば、ISP認証パケットは、ISP P (4) と加入契約をしていないユーザから送られたものかもしれない。あるいは、アクセス局 (7) が、サービスを提供することを必要とせずにISPから補償を得る目的でユーザになりすまして要求を生成することによって、悪意をもってふるまっているかもしれない。そこで、ISP P (4) は、端末U (3) がISP P (4) の真正な加入者であることを確かめるために、端末U (3) の識別(身元)を認証しなければならない。

【0054】端末U (3) を認証するため、ISP P (4) は、端末U (3) によって正しく応答されるとときに端末U (3) の識別を確認することになるチャレンジCH_Pを生成する。注意すべき点であるが、このようなチャレンジは通常、乱数ジェネレータによって生成される大きい数または文字列である。

【0055】この際、ISP P (4) は、ステップ(3a)で端末U (3) によって生成されたチャレンジCH_Uに対する応答も行う。CH_Uは、単に、ISP P (4) の秘密鍵で暗号化されて端末U (3) に送られるだけであるので、端末U (3) は、ISP P (4) の公開鍵を用いてこのメッセージを復号することができる。もとのCH_Uメッセージが判明した場合、端末U (3) には、ISP P (4) の真正が確かめられる(すなわち、ISP P (4) は端末U (3) に認証される)。

【0056】さらに、ISP P (4) は、端末U (3) のセキュリティ要求およびアクセス局A (7) の位置に依存して、信頼ネットワークノードT (5) を選

択する。最後に、ISP_P(4)は、次の内容を有するパケットをアクセス局A(7)に送る。

- ・端末U(3)のチャレンジに対するISP_P(4)の応答。これは、CH_UをISP_P(4)の秘密鍵で暗号化したものである。

- ・端末U(3)を認証するための、ISP_P(4)がランダムに生成したチャレンジCH_P。

- ・信頼ノードT(5)のIPアドレス。

- ・アクセス局A(7)によって端末U(3)に割り当てられたLUID。

【0057】ステップS4bで、アクセス局A(7)は、ISP_P(4)からユーザ認証パケットを受け取ると、修正されたユーザ認証パケットを端末U(3)に転送する。この修正されたユーザ認証パケットは次のものを含む。

- ・端末U(3)のチャレンジに対するISP_P(4)の応答。これは、CH_UをISP_P(4)の秘密鍵で暗号化したものである。

- ・端末U(3)を認証するための、ISP_P(4)がランダムに生成したチャレンジCH_P。

- ・アクセス局A(7)が同時に複数のユーザU(3)にサービスしている場合、端末U(3)に割り当てられたLUIDもユーザ認証パケットに含まれられる。前述のように、LUIDは、どの端末U(3)がデータパケットを受け取るべきかをアクセス局A(7)が判断するのを助ける。

【0058】ステップS5aで、端末U(3)は、ISP_P(4)によってPの公開鍵で暗号化された、チャレンジCH_Uに対するISP_P(4)の応答を、ISP_P(4)の公開鍵を用いて復号し確認する。端末U(3)が、ISP_P(4)の公開鍵を用いて、チャレンジCH_Uに対するISP_P(4)の応答を復号することに成功した場合、端末U(3)には、暗号化された応答が実際にISP_P(4)によって生成されたものであることが確かめられ、これによりISP_P(4)の識別が認証される。

【0059】この時点で、端末U(3)は、端末U(3)の識別を確認し認証するための、ISP_P(4)によって生成されたチャレンジCH_Pに対する応答の生成も行う。ISP_P(4)のチャレンジCH_Pに応答して、端末U(3)は、ISP_P(4)のチャレンジCH_Pを、端末U(3)の秘密鍵で暗号化する。その後、端末U(3)は、次の内容を有するメッセージをアクセス局A(7)に送る。

- ・ISP_PのチャレンジCH_Pに対する端末U(3)の応答。

【0060】ステップS5bにより、アクセス局A(7)は、ステップS5aで生成された端末U(3)からのメッセージを受け取り、それをISP_P(4)に転送する。必ずしも必要ではないが、アクセス局A

(7)が端末U(3)のLUIDをISP_P(4)へのメッセージに含めると有益なことがある。その場合、将来、(ISP_P(4)からアクセス局A(7)を通じて端末U(3)に送らなければならないデータについて)ISP_P(4)が正しい端末U(3)をアクセス局A(7)に指示することが容易になる。

【0061】ステップS6aおよびS6bで、ISP_P(4)は、チャレンジCH_Pに対する端末U(3)の応答が、正当な端末U(3)によって生成されたことを確認する。端末U(3)を認証するために、ISP_P(4)は、チャレンジCH_Pに対する応答を端末U(3)の公開鍵で復号する。復号された応答が、ISP_P(4)のもとのチャレンジCH_Pとなつた場合、ISP_P(4)には、端末U(3)が正当な加入者であり、ISP_P(4)と契約していることが確かめられる。

【0062】ここで、ISP_P(4)は、端末U(3)と信頼ノードT(5)が後で端末U(3)と信頼ノードT(5)の間のトライフィックを暗号化して、端末U(3)と信頼ノードT(5)の間に安全なトンネル(1)を確立するために使用することになるセッション鍵を生成する。セッション鍵とともに、安全なトンネルの有効期間を決定するタイムアウト値が、端末U(3)および信頼ノードT(5)の両方に伝えられる。

【0063】ステップS6aで生成され、ISP_P(4)から信頼ノードT(5)に送られるメッセージは、次の情報を含む。

- ・セッション鍵PT。これは、セッション鍵を、信頼ノードT(5)の公開鍵およびISP_P(4)の秘密鍵で暗号化したものである。注意すべき重要な点であるが、セッション鍵は信頼ノードT(5)の公開鍵で暗号化されるため、信頼ノードT(5)のみが(その秘密鍵を用いて)それを復号することができる。セッション鍵はISP_P(4)の秘密鍵で暗号化されるため、信頼ノードT(5)は、それが実際にISP_P(4)から来たことを(ISP_P(4)の周知の公開鍵を用いて)確認することができる。

- ・安全なトンネル(1)の有効期間を決定するタイムアウト値(詳細は後述)。

- ・アクセス局A(7)のIPアドレス。

- ・アクセス局A(7)によって端末U(3)に割り当てられた、端末U(3)のLUID。

【0064】ステップS6bで生成されたメッセージは、アクセス局A(7)を通じてISP_P(4)から端末U(3)に送られる。すなわち、これは、まずISP_P(4)からアクセス局A(7)に送られた後、アクセス局A(7)によって端末U(3)に転送される。このメッセージは、次の情報を含む。

- ・セッション鍵UT。これは、セッション鍵を、端末U(3)の公開鍵およびISP_P(4)の秘密鍵で暗号

化したものである。注意すべき重要な点であるが、セッション鍵は端末U(3)の公開鍵で暗号化されるため、端末U(3)のみが（その秘密鍵を用いて）それを復号することができる。セッション鍵はISP(4)の秘密鍵で暗号化されるため、端末U(3)は、それが実際にISP(4)から来たことを（ISP(4)の周知の公開鍵を用いて）確認することができる。

・安全なトンネル（1）の有効期間を決定するタイムアウト値。

・アクセス局A(7)によって端末U(3)に割り当てられた、端末U(3)のLUID。注意すべき重要な点であるが、LUIDは、アクセス局A(7)が、メッセージを正しい端末U(3)に転送するためにのみ必要とされる。この情報フィールドは、アクセス局A(7)から端末U(3)に送られる最終的なメッセージでは随意に省略することができる。

【0065】アクセス局A(7)を通じての端末U(3)と信頼ノードT(5)の間の安全なトンネル（1）の生成

いったん端末U(3)およびISP(4)が認証されると、端末U(3)がIPパケットをアクセス局A(7)に送ることができ、さらにそれをアクセス局A(7)が信頼ノードT(5)に転送することができる。また、その逆も可能である（信頼ノードT(5)がIPパケットをアクセス局A(7)に送ることができ、その後それをアクセス局A(7)が端末U(3)に転送することができる）。その結果、端末U(3)と信頼ノードT(5)の間に（アクセス局A(7)を通じて）安全なトンネル（1）が確立される。この安全なトンネル（1）の目的は、端末U(3)と信頼ノードT(5)の間の物理リンクをエミュレートすることである。さらに、端末U(3)および信頼ノードT(5)は両方とも（ISP(4)によって生成された）同じセッション鍵を有するため、安全なトンネル（1）を通るトライックはこのセッション鍵で暗号化することができる。安全なトンネルを通るパケットを暗号化することにより、端末U(3)と信頼ノードT(5)の間に位置するネットワーク要素（例えば、アクセス局A(7)）は、端末U(3)や信頼ノードT(5)によって検出されずにIPパケットの追加、変更あるいは除去を行うことは不可能となる。

【0066】アクセス局A(7)は、メッセージを信頼ノードT(5)に送るときにはいつも、そのメッセージを発信した端末U(3)のLUIDを含める。LUIDは、アクセス局A(7)のIPアドレスとともに、信頼ノードT(5)が端末U(3)を識別するために使用可能なグローバルに一意的なIDを生成する。

【0067】さらに、信頼ノードT(5)は、（端末U(3)への最終的配送のために）アクセス局A(7)に送るのと同じLUIDをメッセージに含める。アクセ

局A(7)は、このLUIDを用いて、メッセージの転送先とすべき正しい端末U(3)を決定することができる。LUIDは、端末U(3)にとっては重要でないため、アクセス局A(7)は、信頼ノードT(5)から端末U(3)に転送するメッセージからそれを随意に除去することも可能である。

【0068】端末UとIPネットワークの間のデータ転送

次に、図2および図5を参照して、端末U(3)とIPネットワーク（9）（例えば、インターネットや社内インターネット）の間のデータ転送について説明する。注意すべき重要な点であるが、図4が、端末U(3)、アクセス局A(7)、ISP(4)、および信頼ノードT(5)の間のメッセージシーケンスを示したのとは異なり、図5は、端末U(3)、アクセス局A(7)、信頼ノードT(5)およびインターネット（9）の間のメッセージシーケンスを示す。

【0069】図5から理解されるとともに、すでに説明したように、端末U(3)と信頼ネットワークノードT(5)の間でアクセス局A(7)を通じてデータを送信するために、安全なトンネル（1）が確立される。端末U(3)、アクセス局A(7)、および信頼ノードT(5)が安全なトンネル（1）を通じてIPパケットを交換することができることにより、これ以上ISP(4)が関与することは不要となる（ISP(4)の関与は、生成されたセッション鍵が端末U(3)および信頼ノードT(5)に安全に配送されたときに終了する）。

【0070】一般に、安全なトンネル（1）を通じてIPパケットを送信する前に、端末U(3)は、信頼ノードT(5)からIPアドレスを取得するために、安全なトンネル（1）を通じて第2のDHCP要求を信頼ノードT(5)に転送する。注意すべき重要な点であるが、安全なトンネル（1）は、端末U(3)と信頼ノードT(5)の間の物理リンクをエミュレートする。安全なトンネル（1）が確立された後、端末U(3)は次の2つのネットワークインターフェースを有する（それぞれIPアドレスを必要とする）。

【0071】1) 端末U(3)をアクセス局A(7)と接続する物理インターフェース（例えば、イーサーネットカードや802.11ワイヤレスLANカード）。端末U(3)は、第1のDHCP要求を送出することによって、このインターフェースに対するIPアドレスを取得した。このDHCP要求は、アクセス局A(7)によって受信され応答された。

【0072】2) 端末U(3)を信頼ノードT(5)と接続する、安全なトンネル（1）への論理インターフェース。端末U(3)は、安全なトンネル（1）を通じて第2のDHCP要求をブロードキャストすることによって、このインターフェースに対する別のIPアドレスを取

得しなければならない。ただし、この第2のDHC P要求は、信頼ノードT (5) によって受信され応答される。

【0073】第2のIPアドレスを信頼ノードT (5) から取得することにより、端末U (3) は、グローバルインターネット (9) によって信頼ノードT (5) へとルーティングされる送信元アドレスを有するIPパケットを生成することが可能となる。さらに、信頼ノードT (5) は、その宛先アドレスを有するIPパケットを、信頼ノードT (5) と端末U (3) の間のトンネルを通じて端末U (3) に転送することが可能となる。

【0074】第2のDHC P要求に関するメカニズムについて以下で説明する。端末U (3) は、(自分(端末U (3))と信頼ノードT (5)との間に確立した)安全なトンネル(1)を、追加の(論理)ネットワークインターフェースとして利用可能にするために、第2のDHC P要求を生成する。ステップ7aに示すように、端末U (3) は、このDHC P要求を、端末U (3) と信頼ノードT (5) の間で共有されるセッション鍵で暗号化する。次に、端末U (3) は、暗号化されたDHC P要求を、新たなIPパケット「Y」のペイロードフィールドに入れる(すなわち、Y [DHC P要求/セッション鍵])。「Y」IPパケットは、信頼ノードT (5) のIPアドレスをその宛先アドレスとし、アクセス局A (7) のアドレスをその送信元アドレスとする。「Y」IPパケット(Y [DHC P要求/セッション鍵])は、アクセス局A (7) に転送される。アクセス局A (7) は、「Y」IPパケットを信頼ノードT (5) に転送するが、パケット内の内容を復号することはできない。アクセス局A (7) は正しいセッション鍵を有しないからである。注意すべき重要な点であるが、アクセス局A (7) は、「Y」IPパケットを信頼ノードT (5) に転送するときに、前述したように、端末U (3) のLUIDを「Y」IPパケットに付加することが可能である。

【0075】ステップS7bにおいて、信頼ノードT (5) は、アクセス局A (7) を通じて、暗号化されたDHC P要求を含む「Y」IPパケットを端末U (3) から受け取ると、DHC P要求を復元し、IPアドレスを端末U (3) に割り当て、端末U (3) に対するDHC P応答を生成する。明らかなように、このDHC P要求によって端末U (3) に割り当てられるIPアドレスは、グローバルインターネット (9) がメッセージを信頼ノードT (5) にルーティングするために使用するIPアドレスである。その後、このDHC P応答は、セッション鍵で暗号化されてアクセス局A (7) に転送され、アクセス局A (7) はこの応答を端末U (3) に送る。この間、アクセス局A (7) は応答の内容を復号することはできない。

【0076】端末U (3) は、暗号化されたDHC P応

答を受け取ると、IPアドレスを取得する。このIPアドレスは、グローバルインターネット (9) が信頼ノードT (5) にルーティングし、信頼ノードT (5) が端末U (3) に(アクセス局A (7) を通じての、安全なトンネル(1)を通じて)転送するものである。明確にするため、注意すべき点であるが、上記のDHC P応答に含まれるIPアドレスは、信頼ノードT (5) 自体のIPアドレスではなく、グローバルインターネット (9) が信頼ノードT (5) にルーティングするIPアドレスである。信頼ノードT (5) は、このIPアドレスを宛先アドレスとして有するメッセージを受け取ると、信頼ノードT (5) がメッセージの最終受信者ではなく、端末U (3) である最終宛先へメッセージを転送することになっていることを容易に判断することができる(すなわち、信頼ノードT (5) はルータとして作用する)。信頼ノードT (5) は、端末U (3) のDHC P要求に対して、前記IPアドレスを含むDHC P応答により応答するとき、前記IPアドレスを端末U (3) の識別および対応するアクセス局A (7) と関連づけるコードを保持する。この情報により、信頼ノードT (5) は、グローバルインターネット (9) から受け取るあらゆるIPパケットについて、次の情報を判定することが可能となる。

- ・パケットの転送先となるべき関連づけられた端末U (3)。
- ・信頼ノードT (5) をその特定の端末U (3) と接続する安全なトンネル(1)。
- ・安全なトンネル(1)を通じての送信用にパケットを暗号化するために使用しなければならないセッション鍵。
- ・安全なトンネル(1)が通り、暗号化されたパケットの転送先となるべき、関連づけられたアクセス局A (7)。

【0077】ステップS8aにおいて、端末U (3) と信頼ノードT (5) との間の(安全なトンネル(1)を通じて)パケットトラフィックの送信について詳細に説明する。この説明は、データパケットの詳細な内訳を示す図3を参照することにより補足される。具体的には、端末U (3) は、新たなIPパケットX (11) を作成する。図3からわかるように、データパケットX (11) のパケットヘッダ(12)は、リモートホストR (10) (図1に示されるような)の宛先アドレスと、端末U (3) からという送信元アドレスを有する。特に、送信元アドレスは、端末U (3) の要求に対して信頼ノードT (5) から端末U (3) に返されるDHC P IPアドレスである。

【0078】次に、IPパケット(11)全体(データパケットXおよびヘッダを含む)が、端末U (3) と信頼ノードT (5) の間で共有されるセッション鍵で暗号化され、データパケットY (16) のペイロード(1

4) として格納される (Y [X/k e y])。ここで、暗号化されたIPパケットY [X/k e y] (16) のヘッダ (18) 宛先アドレスは、信頼ノードT (5) のIPアドレスであり、このIPパケットの送信元アドレスは、端末U (3) に割り当てられるマジックDHCPアドレスである。

【0079】ステップS8aに示されるように、アクセス局A (7) は、暗号化されたIPパケットY [X/k e y] (16) を受信する。アクセス局A (7) は、もちろん、暗号化されたIPパケットY [X/k e y] (16) 内に含まれる内容 (すなわちX) を復元したり操作したりすることはできない。そこで、アクセス局A (7) は、暗号化されたIPパケットY [X/k e y] (16) 内の送信元アドレスフィールドをアクセス局A (7) のIPアドレスで置き換えて、修正されたパケットY' [X/k e y] を作成することにより、暗号化されたIPパケットY [X/k e y] (16) を信頼ノードT (5) に転送する。さらに、アクセス局A (7) は、どの端末U (3) がもとのパケットX (11) を送信したかを信頼ノードT (5) が判断するのを助けるために、端末U (3) のLUIDを修正されたIPパケットY' [X/k e y] に付加することが可能である。信頼ノードT (5) は、メッセージを復号する正しいセッション鍵を選択するためには、どの端末U (3) がパケット (11) を送信したかを知らなければならない。

【0080】ステップS8bにより、信頼ノードT (5) は、もとのデータパケットX (11) を復元する。データパケットX (11) はインターネット (9) に転送される。同様に、端末U (3) 宛のインターネット (9) からのデータパケットは、ステップS8bに示されるように、信頼ノードT (5) によって受信される。信頼ノードT (5) は、セッション鍵を用いてデータパケットを暗号化した後、ステップS8aに示されるように、暗号化されたパケットをアクセス局A (7) に転送する。アクセス局A (7) は、LUIDに基づいて、メッセージを正しい端末U (3) に転送する。

【0081】別法として、IP送信元アドレスと送信元ポート番号の一意的な2つ組をトンネルにマッピングするNAT (ネットワークアドレス変換) メカニズムが使用される場合には、ステップS7を省略することも可能である。その場合、端末U (3) によって送信され信頼ノードT (5) によって受信される最初のデータパケットX (11) が、端末U (3) を信頼ノードT (5) と関連づけることになる。そして、トンネルと外部インターネット接続との間で接続パラメータをマッピングするデータ構造が作成される。

【0082】トンネル解放とタイムアウト

タイムアウトメカニズムは、端末U (3) と信頼ノードT (5) の間に確立された安全なトンネル (1) に関するリソースの解放をトリガする。前記リソースは、端

末U (3) 、アクセス局A (7) および信頼ノードT (5) に存在する。タイムアウトおよびトンネル解放を制御するタイミングメカニズムは、トンネルの両端 (すなわち、端末U (3) 内および信頼ノードT (5) 内) に配置されることが可能である。タイミングメカニズムは、端末U (3) および信頼ノードT (5) へのセッション鍵の配送の成功時にセットされる。それぞれのタイミングメカニズムのタイム値は、ISP P (4) と端末U (3) の間、およびISP P (4) と信頼ノードT (5) の間で転送されるセッション鍵とともに渡されることが可能である。

【0083】端末U (3) へのサービス提供と、提供される関連リソースとを制御する別個のタイマが、アクセス局A (7) で維持される。このタイマは、トンネル (1) が確立されると、すなわち、セッション鍵が転送されるとすぐに開始される。好ましくは、端末U (3) 宛のタイムアウト値が、このタイマのプリセット値として使用される。タイムアウト時に、サービス提供は停止され、アクセス局A (7) におけるリソースは解放される。正しい動作を保証するため、データ転送の場合であっても、アクセス局A (7) にあるタイマのタイムアウト値は、トンネル (1) のタイムアウトのタイムアウト値より大きくすべきである。

【0084】トンネル (1) の有効期間を延長するためには、端末U (3) は、タイマが満期になる前に、新たなサービスおよびISP P (4) との再認証要求を呼び出すことが可能である。再認証要求は、アクセス局A (7) によって端末U (3) に提供される接続サービスについて、端末U (3) の真正と、計測された継続時間情報を保証する。端末U (3) および信頼ノードT (5) にあるタイマが満期になると、トンネルリソースは、それぞれのネットワーク要素から解放される。

【0085】しかし、遅いデータ転送中のトンネルの正しい動作および維持を保証するために、各タイマは、安全時間マージン(safety time margin)を有することも可能である。安全時間マージンは、タイマに追加時間のバッファを割り当てることにより、リソースが解放されたり再認証要求がなされたりする前に、遅いデータ転送が完了するようになる。

【0086】課金

アクセス局A (7) が端末U (3) にサービスを提供した時間の長さに基づくアカウンティング方法も実現される。ある計測単位を利用して、アクセス局A (7) が端末U (3) にサービスを提供した期間を計上する。計測単位は、端末U (3) 、信頼ノードT (5) およびアクセス局A (7) に渡されるタイムアウト値によって決定される。計測単位は、数十秒から数分までの範囲にある時間単位とすることが可能である。通常、計測単位は、ISP P (4) とアクセス局A (7) の間のサービス契約、および、ISP P (4) と端末U (3) の間の

契約によって規定される。タイムアウト値は、再認証手続きの呼出しによって引き起こされる時間粒度とシグナリングおよび処理のオーバーヘッドとによって影響を受けることがある。タイミングメカニズムは、システムの正しい動作にとって必要であるため、課金情報は、定期的な再認証手続き中に伝達されるタイムアウト値から導出することが可能である。

【0087】ISP P (4) が、端末U (3) によって利用されたリソースについてアクセス局A (7) に補償するとともにタイマ値に基づいて端末U (3) に課金するように、タイマ値はISP P (4) によって生成され配送されることも可能であるが、端末U (3) が、プリペイドオプションによりISPサービスを取得することも可能である。例えば、端末U (3) は、与えられた期間tの間だけ、アクセス局A (7) により提供されるリソースに端末U (3) がアクセスしそれを利用する許可するプリペイド加入契約をISP P (4) と結ぶことが可能である。期間tは、ISP P (4) から端末U (3) が購入する計測単位(例えば分単位)の量に対応する。通常、それぞれの認証および再認証の成功により、タイムアウト間隔(例えば1分)と等価な金額分がデクリメントされる。プリペイド時間単位が使い果たされると、ISP P (4) は、端末U (3) に対して、再認証や新たなタイムアウト値の配達を行わない。その後、アクセス局A (7)、信頼ノードT (5) および端末U (3) にあるタイマが満期になり、トンネル(1)は関連するリソースとともに解放される。

【0088】

【発明の効果】以上説明したように、本発明によれば、端末と第三者所有の信頼されない(非信頼)アクセス局との間に接続を確立し、続いて、端末と契約しているインターネットサービスプロバイダ(ISP)へISP認証要求を送信する。ISPと端末が正しく認証された後、端末と信頼ゲートウェイとの間に信頼された接続を確立する。こうして確立された接続を安全なトンネルとして利用することにより、ISPは、非信頼アクセス局を通じて端末に対して安全なインターネットアクセスを提供することができる。

【0089】こうして公衆インターネットやプライベートLANのようなパブリックまたはプライベートIPネ

ットワークへのアクセスのために、既存のインフラストラクチャの共有を可能にするメカニズムを提供することができる。特に、インフラストラクチャの所有者はそのリソースを異なるISPへ短期間ベースでリースし、1つのISPはこれらリソースを用いて加入者にインターネットサービスを提供する。ISPは、課金、帯域管理およびeメールなど、加入者に提供されるインターネットサービスの全ての側面を制御する。また、ISPは暗号化によって、加入者のプライバシーを保証する。既存のネットワーク・インフラストラクチャからのネットワークリソースのリースによって、ISPにとっては高価なアクセスインフラ自体を構築する必要がなくなり、他方、インフラストラクチャの所有者にとってはインフラから付加的な報酬を発生させる機会が与えられる。重要なのは、ユーザにとってもISPにとっても、IPネットワークへのアクセスを実行するためのアクセス局を信頼する必要がない(すなわちアクセス局は非信頼である)ことである。

【図面の簡単な説明】

【図1】本発明によるネットワークのモデルを示す図である。

【図2】本発明の実施例のコンポーネント間の情報フローを示す図である。

【図3】アクセス局Aを通じてユーザ(U)から信頼ネットワーク要素Tに転送されるトンネル化データパケットを示す図である。

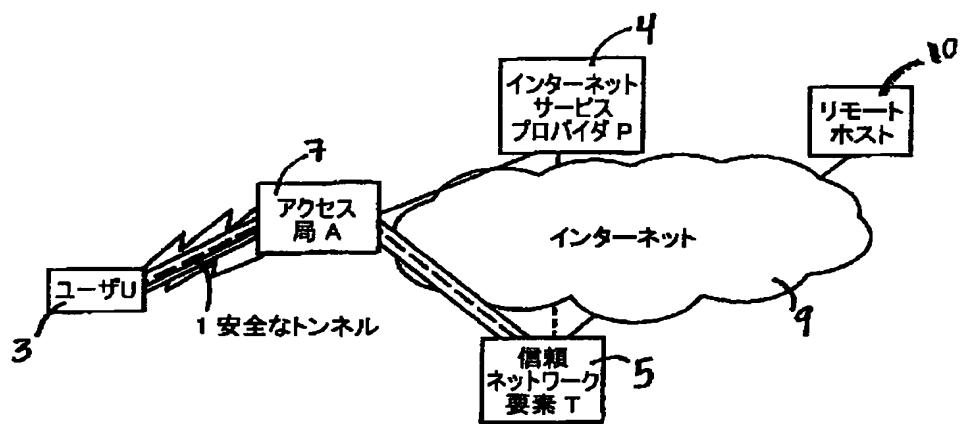
【図4】セッション鍵の認証および配送のメッセージシーケンスを示す図である。

【図5】アソシエーションおよびデータ転送のメッセージシーケンスを示す図である。

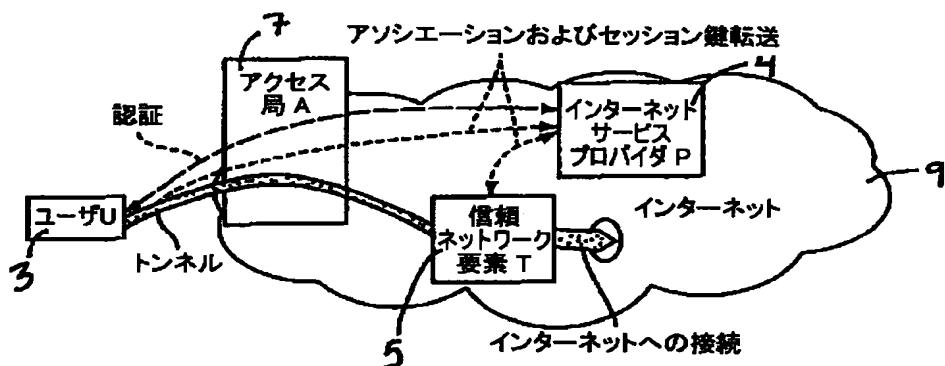
【符号の説明】

- 1 安全なトンネル
- 3 端末ユーザU
- 4 ISP P
- 5 信頼ノードT
- 7 アクセス局A
- 9 IPネットワーク
- 10 リモートホスト
- 11 データパケットX
- 16 データパケットY

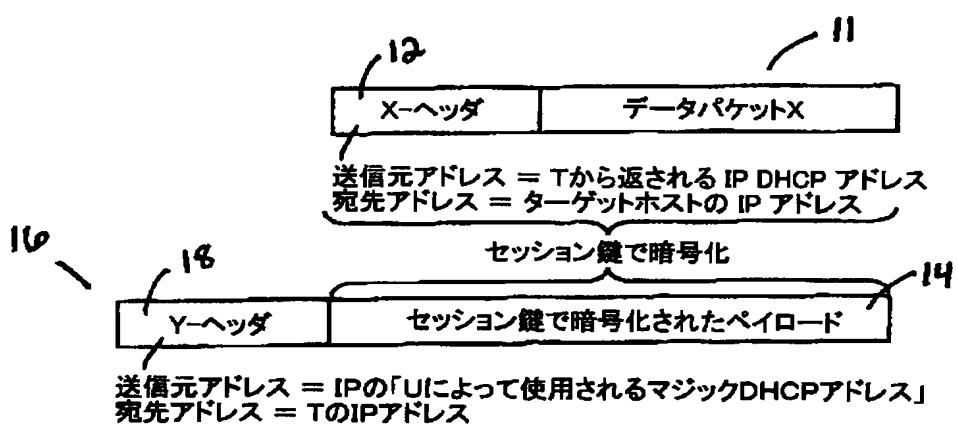
【図1】



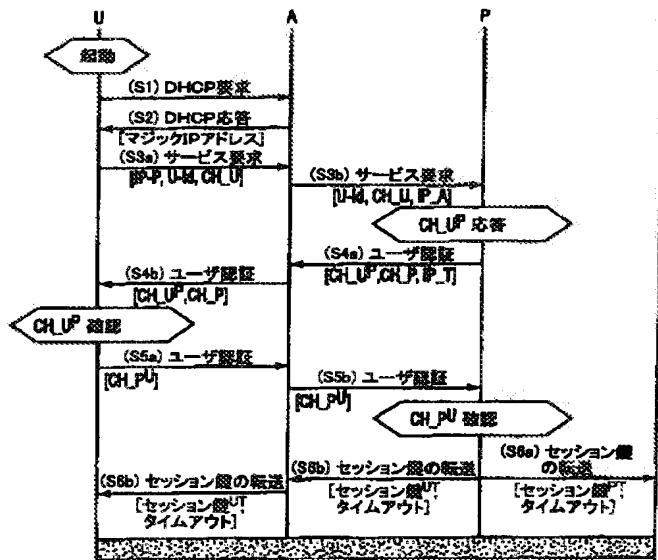
【図2】



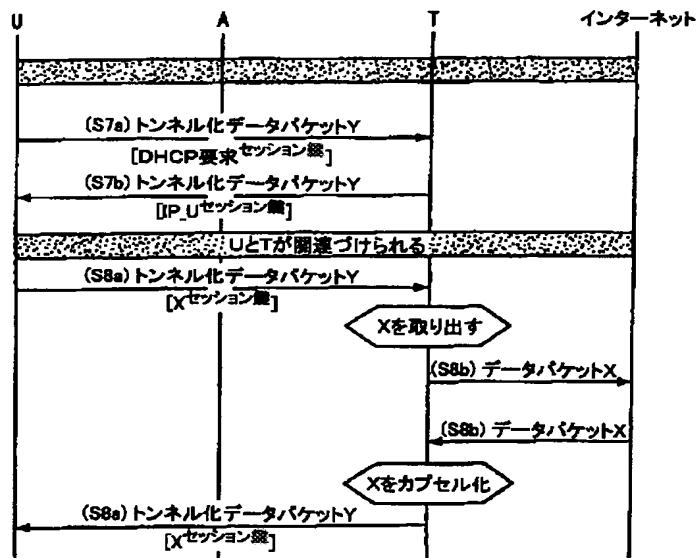
【図3】



【図4】



【図5】



フロントページの続き

(51) Int. Cl. 7

H 04 L 12/56
H 04 Q 7/38

識別記号

F I

H 04 L 9/00
H 04 B 7/26

マークコード (参考)

601B
109R

(72)発明者 トーマス クーネル
アメリカ合衆国, ニュージャージー
08540 プリンストン, 4 インディペン
デンス ウエイ, エヌ・イー・シー・ユ
ー・エス・エー インク内

(72)発明者 ワルフ ミューラー
アメリカ合衆国, ニュージャージー
08540 プリンストン, 4 インディペン
デンス ウエイ, エヌ・イー・シー・ユ
ー・エス・エー インク内
Fターム(参考) 5B085 AC04 AE01 AE29 BA06 BG02
BG07
5B089 GB01 HB18 KA17 KB13
5J104 AA07 KA02 NA03 PA07
5K030 GA15 HA08 HD09 KX24 LC15
LD19
5K067 AA30 BB21 DD11 DD17 EE02
HH23 HH36

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-023420
(43)Date of publication of application : 24.01.2003

(51)Int.Cl. H04L 9/08
G06F 13/00
G06F 15/00
G09C 1/00
H04L 12/56
H04Q 7/38

(21)Application number : 2002-069405 (71)Applicant : NEC CORP
(22)Date of filing : 14.03.2002 (72)Inventor : REDLICH JENS-PETER
KUEHNEL THOMAS
MUELLER WOLF

(30)Priority
Priority number : 2001 278436 Priority date : 26.03.2001 Priority country : US
2002 057914 29.01.2002 US

(54) COMMUNICATION METHOD THROUGH INTERMEDIARY OF UNTRUSTED ACCESS STATIONS

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a mechanism that enables sharing of the existing infrastructure for accessing public or private IP networks, such as the public Internet or private LANs.

SOLUTION: The method of this invention includes the steps of establishing a connection between a terminal U and an untrusted access station A, transmitting a user authentication request to an internet service provider (ISP) P which is contracted with the terminal U, and establishing a trusted association between the terminal U and a trusted gateway T upon correct authentication of the ISP P and the terminal U. Through such an established secure tunnel, the ISP P can dynamically acquire control of resources by the access station A, in order to provide a prescribed service to the terminal U. After the legal authentication between the terminal U and the ISP P, the ISP P can generate a session key to encrypt data packets.

